#3

Patent
Attorney's Docket No. 019952-157

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Hideyuki TORII	)	Group Art Unit: 2167
	)	
Application No.: 09/819,814	)	Examiner: Unassigned
	)	
Filed: March 29, 2001	)	
	)	
For: ASSETS MANAGEMENT METHOD AND SYSTEM	)	
	)	

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

Japanese Patent Application No. 2000-199276

Filed: June 30, 2000.

In support of this claim, enclosed is a certified copy of the prior foreign application. This application is referred to in the oath or declaration. Acknowledgment of receipt of this certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: July 9, 2001

By: William C Rowland RN 30888, for
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

(Translation of the front page
of the priority document of
Japanese Patent Application
No. 2000-199276)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application : June 30, 2000

Application Number : Patent Application
2000-199276

Applicant(s) : NUMERICAL TECHNOLOGIES KABUSHIKI KAISHA

May 11, 2001

Commissioner,

Patent Office Kouzo OIKAWA

Certification Number 2001-3037570

P201-0062

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　６月３０日

出願番号
Application Number: 特願２０００－１９９２７６

出願人
Applicant(s): ニューメリカルテクノロジーズ株式会社

２００１年　５月１１日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０３７５７０

【書類名】　特許願

【整理番号】　2000P0901

【提出日】　平成12年 6月30日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/00

【発明の名称】　資産管理方法及びそのシステム

【請求項の数】　12

【発明者】

【住所又は居所】　東京都文京区本郷３丁目４２番５号ボア本郷４階　ニューメリカルテクノロジーズ株式会社内

【氏名】　鳥居　秀行

【特許出願人】

【住所又は居所】　東京都文京区本郷３丁目４２番５号ボア本郷４階

【氏名又は名称】　ニューメリカルテクノロジーズ株式会社

【代表者】　鳥居　秀行

【代理人】

【識別番号】　100076428

【弁理士】

【氏名又は名称】　大塚　康徳

【電話番号】　03-5276-3241

【選任した代理人】

【識別番号】　100101306

【弁理士】

【氏名又は名称】　丸山　幸雄

【電話番号】　03-5276-3241

【選任した代理人】

【識別番号】　100115071

【弁理士】

【氏名又は名称】　大塚　康弘

【電話番号】　03-5276-3241

【手数料の表示】

【予納台帳番号】　003458

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　資産管理方法及びそのシステム

【特許請求の範囲】

【請求項１】　資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置に、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段を設けて、使用者の資源へのアクセスを管理し、

不特定多数の利用者による、ネットワークを介した前記リスク収益管理装置へのアクセスを可能とすることを特徴とする資産管理方法。

【請求項２】　前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与することを特徴とする請求項１記載の資産管理方法。

【請求項３】　前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化されることを特徴とする請求項１記載の資産管理方法。

【請求項４】　資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置と、ネットワークを介して前記リスク収益管理装置にアクセスする利用者端末とを含む資産管理システムであって、

前記リスク収益管理装置に、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段を設けて、使用者の資源へのアクセスを管理し、

不特定多数の利用者による、ネットワークを介した前記リスク収益管理装置へのアクセスを可能とすることを特徴とする資産管理システム。

【請求項５】　前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与することを特徴とする請求項４記載の資産管理システム。

【請求項６】　前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化されることを特徴とする請求項４記載の資産管理システム。

【請求項７】　利用者又は管理対象資産毎の入出力データを格納及び検索す

るデータ管理手段と、

該入力データを処理し出力データを得る計算処理手段と、

利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段と、

フロー制御とデータ暗号化とデータ圧縮展開を行うネットワーク接続管理手段とを備えることを特徴とするリスク収益管理装置。

【請求項８】　前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与することを特徴とする請求項７記載のリスク収益管理装置。

【請求項９】　前記ネットワーク接続管理手段は、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化することを特徴とする請求項７記載のリスク収益管理装置。

【請求項１０】　資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置を制御する制御プログラムをコンピュータ読み取り可能に記憶する記憶媒体であって、

前記制御プログラムが、

利用者又は管理対象資産毎の入出力データを格納及び検索するデータ管理プログラムと、

該入力データを処理し出力データを得る計算処理プログラムと、

利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理プログラムと、

フロー制御とデータ暗号化とデータ圧縮展開を行うネットワーク接続管理プログラムとを含むことを特徴とする記憶媒体。

【請求項１１】　前記履歴認証管理プログラムは、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与するステップを含むことを特徴とする請求項１０記載の記憶媒体。

【請求項１２】　前記ネットワーク接続管理プログラムは、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化するステップを含むことを特徴とする請求項１０記載の記憶媒体。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】

本発明は、地理的に分散した利用者及び管理対象資産のデータを対象として、効率的かつ安全な資産のリスク管理及び収益管理を可能とする資産管理方法及びそのシステムに関するものである。

【０００２】

【従来の技術】

従来のこの種の方法及びシステムでは、資産のリスク管理及び収益管理を可能とするために、管理対象資産の入力データ管理部と、該入力データから計算結果を得る計算処理部と、該計算結果の格納及び検索を行う出力データ管理部と、利用者に実際の機能を提供するユーザインタフェース部とを、１つの一体化したシステムとして構築するか、あるいは相互に緊密にネットワーク接続したシステムとして構築しており、処理できる管理対象資産は小規模であった。

【０００３】

これは、顧客情報や信用情報が含まれるなど機密性の高い金融データが外部に流出する危険を避けるため、同一の企業体内での利用あるいは機密性の低い情報の分析に用途が限定されていたためである。

【０００４】

しかしながら、昨今、データ量が大きな大手事業法人や金融機関規模の資産に対してリスク管理及び収益管理機能を提供することが求められており、その為には、広帯域かつ信頼性の高いネットワーク間通信が必要となる。

【０００５】

この要求を実現するためには、従来のシステムでは、地理的に分散した利用者及び管理対象資産のデータが対象の場合に、インターネット接続に代表されるようなネットワークは、安価な反面、帯域が限定される又は信頼性の乏しいため、利用することが困難であった。

【０００６】

又、従来のシステムでは、バリュー・アット・リスク（ＶａＲ）、リスク・リターン分析、ポートフォリオ最適化など、個別の方法論において様々な見解や手

法の相違が含まれるポートフォリオ理論を適用しようとした場合、利用者又は管理対象資産毎に別々の方式や異なる基準を提供することが困難であった。

【０００７】

更に、従来のシステムでは、持続的な機能向上や改定を行う場合には利用者端末側の装置又はソフトウェアを変更する必要があり、稼動後の機能の変更が難しく、変更をするには維持コストの上昇を招いていた。

【０００８】

【発明が解決しようとする課題】

本発明は、上記従来の欠点を除去し、地理的に分散した利用者及び管理対象資産のデータを対象にした、安価で融通性に富み、信頼性の高い、効率的かつ安全な資産のリスク管理及び収益管理を可能とする資産管理方法及びそのシステムを提供する。

【０００９】

【課題を解決するための手段】

上述した課題を解決するために、本発明の資産管理方法は、資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置に、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段を設けて、使用者の資源へのアクセスを管理し、不特定多数の利用者による、ネットワークを介した前記リスク収益管理装置へのアクセスを可能とすることを特徴とする。ここで、前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与する。また、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化される。

【００１０】

又、本発明の資産管理システムは、資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置と、ネットワークを介して前記リスク収益管理装置にアクセスする利用者端末とを含む資産管理システムであって、前記リスク収益管理装置に、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段を設けて、使用者の資源へのアクセスを管理し

、不特定多数の利用者による、ネットワークを介した前記リスク収益管理装置へのアクセスを可能とすることを特徴とする。ここで、前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与する。また、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化される。

【００１１】

又、本発明のリスク収益管理装置は、利用者又は管理対象資産毎の入出力データを格納及び検索するデータ管理手段と、該入力データを処理し出力データを得る計算処理手段と、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理手段と、フロー制御とデータ暗号化とデータ圧縮展開を行うネットワーク接続管理手段とを備えることを特徴とする。ここで、前記履歴認証管理手段は、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与する。又、前記ネットワーク接続管理手段は、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化する。

【００１２】

又、本発明に記憶媒体は、資産に関する入力データを計算してリスク管理及び収益管理のデータを作成するリスク収益管理装置を制御する制御プログラムをコンピュータ読み取り可能に記憶する記憶媒体であって、前記制御プログラムが、利用者又は管理対象資産毎の入出力データを格納及び検索するデータ管理プログラムと、該入力データを処理し出力データを得る計算処理プログラムと、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理プログラムと、フロー制御とデータ暗号化とデータ圧縮展開を行うネットワーク接続管理プログラムとを含むことを特徴とする。ここで、前記履歴認証管理プログラムは、利用者又は管理対象資産に基づいてリスク収益管理装置の資源を利用する権限を付与するステップを含む。又、前記ネットワーク接続管理プログラムは、前記利用者とリスク収益管理装置との間でネットワークを介して伝送されるデータは、機密性に応じて暗号化するステップを含む。

【００１３】

上記構成により、利用者の手元からシステムを制御し、データの入出力を行い、処理結果を表示する方法を提供するものである。

【００１４】

又、利用者端末との間でやりとりするデータを圧縮し、暗号化し、かつ利用者毎又は管理対象資産毎に認証キーを付加し、低容量の回線使用下でも大容量データを入出力する利便性とセキュリティを提供するものである。

【００１５】

又、利用者毎又は管理対象資産毎に記憶領域を持ち、利用者又は管理対象資産毎に別々の方式や異なる基準に基づく出力結果を抽出して提供するものである。

【００１６】

又、地理的に分散あるいは複数になりうる利用者端末側ではなく、集中された拠点に配置されるため、容易な機能改定と維持コストを実現するものである。

【００１７】

【発明の実施の形態】

次に、本発明の実施の形態について、添付図面を参照して説明する。

【００１８】

＜本実施の形態の資産管理システムの構成例＞

図１は、本発明の一実施の形態のシステムを示すブロック構成図である。

【００１９】

図において、１は、利用者又は管理対象資産毎の入出力データを格納及び検索するデータ管理部、２は、データ管理部１及びネットワークからの入力データを処理し出力データを得る計算処理部、３は、利用者又は管理対象資産毎の履歴及び認証管理を行う履歴認証管理部、４は、フロー制御とデータ暗号化とデータ圧縮展開とを行うネットワーク接続管理部であり、これらデータ管理部１と計算処理部２と履歴認証管理部３とネットワーク接続管理部４とで、リスク収益管理装置を構成する。尚、本例ではリスク収益管理装置を構成する各構成要素をネットワーク接続管理部４に接続する構成で示したが、データ管理部１と計算処理部２と履歴認証管理部３がネットワーク上に分散して配置されていても、あるいはＬＡＮなどの構内ネットワークで接続されていても構わない。

【００２０】

５は、地理的に分散した複数の利用者又は管理対象資産のデータを結ぶネットワーク回線であり、インターネット、公衆回線接続、又は専用ネットワークを含む。６は、システムを制御し、データの入出力を行い、処理結果を表示する利用者端末である。利用者端末６は複数存在し、地理的に散在していて構わない。すなわち、利用者端末６は、金融機関にあっても、一般の個人の所有であっても構わず、誰もが本システムに参入することが可能である。

【００２１】

図２は、上記のような本システムを実現するためのハードウエア構成例を示す図である。図２において、図１と対応する要素は同じ参照番号を付与している。

【００２２】

図２において、１はデータ管理部であり、資産データが利用者及び／又は管理対象資産毎に管理されて格納されているデータ管理データベース（ＤＢ）１ａと、そのデータ管理プログラム１ｂとを含む。２は計算処理部に対応する資産変動などを計算する計算処理プログラム、３は履歴認証管理部であり、利用者単位でその履歴及び認証キーを格納する履歴認証キーデータベース（ＤＢ）３ａと、履歴認証を実行する履歴認証プログラム３ｂとを含む。４はネットワーク接続管理部であり、ネットワークを介して送信されるデータを圧縮し、受信されたデータを展開するデータ圧縮展開プログラム４ａと、ネットワークを介する通信接続のプロトコル等の実行、及びデータの暗号化／復号を実行する接続応答・暗号化プログラム４ｂとを含む。これらのデータ及びプログラムは、ハードディスクやフロッピーディスクなどの磁気ディスクや、ＣＤ－ＲＯＭ，ＣＤ－ＲＷやＤＶＤなどの光ディスク、メモリカード等の大容量の記憶装置に格納されており、主記憶装置２１にロードして実行される。

【００２３】

リスク収益管理装置側で、７はキーボード装置であり、リスク収益管理装置の起動・停止・監視などの操作を行う。８はディスプレイ装置であり、キーボード装置７の操作に応じてリスク収益管理装置の状態を表示する。２１は、上記記憶装置からデータ及びプログラムをロードしたり、計算処理時に一時記憶として使

用される主記憶装置、２２は主記憶装置２１にロードされたプログラムにより、リスク収益管理装置全体を制御する制御装置、２３は計算処理プログラム２に従って特殊な計算を高速で行うように用意された演算装置である。尚、制御装置２２と演算装置２３は、汎用コンピュータでは１つのＣＰＵで実現されるし、特殊コンピュータでは並列動作する複数のＣＰＵに分配されている。

【００２４】

５はネットワーク回線であり、利用者端末６側にはネットワーク接続装置５ａ、リスク収益管理装置側にはネットワーク接続装置５ｂが配置されている。

【００２５】

利用者端末６において、９は、利用者端末のキーボード装置であり、リスク収益管理装置側に対して、バリュー・アット・リスク（ＶａＲ）、リスク・リターン分析、ポートフォリオ最適化などの計算実行、データ転送、結果照会などをコマンド操作したり認証データなどを入力する。１０は、利用者端末のディスプレイ装置であり、キーボード装置７の操作に応じてリスク収益管理装置が返した応答及び各種制御表示プログラム１５で解析処理された結果を表示する。１１は、利用者端末６全体を制御する制御装置、１２は、利用者端末上で各種演算処理を行う演算装置である。尚、利用者端末６は誰でも本システムに参入できるように汎用コンピュータが好ましく、一般に制御装置１１と演算装置１２とは１つのＣＰＵで実現される。

【００２６】

２０は記憶装置であり、以下のデータ及びプログラムが記憶されている。１３はデータ圧縮展開プログラムで、リスク収益管理装置のネットワーク接続管理部４との間で送受するネットワーク回線５を流れるデータの圧縮と展開を行う。１４はデータ暗号化プログラムで、リスク収益管理装置のネットワーク接続管理部４との間で送受するネットワーク回線５を流れるデータの暗号化を行う。１５は、利用者端末における各種の制御表示を行う各種制御表示プログラムである。１６は、ネットワーク回線５を介してデータ管理部１に送られるまで一時滞留する資産データ記憶部である。

【００２７】

＜本実施の形態の履歴認証の構成例＞

図３は、履歴認証キーＤＢ３ａの一構成例を示す図である。

【００２８】

利用者端末６から送信されたデータには、少なくとも端末ＩＤ、利用者ＩＤ（パスワード等を含む）、履歴認証キーが含まれており、これらに基づき履歴認証キーＤＢ３ａの端末ＩＤ３１、利用者ＩＤ３２、履歴認証キー３３を検索して、一致するものを探す。一致するものが無ければリスク収益管理装置は利用者端末６からの要求を受付けない。一致するものがあれば、入力データ制限３４、計算処理制限３５、出力データ制限３６に基づいて、その利用者が利用できる資源及び提供するサービスを制限する。例えば、この制限は、同じ金融機関からか、他の金融機関からか、あるいは一般の顧客からか、更に顧客であれば、取引高や取引継続年月などに基づいて、決定されればよい。尚、端末ＩＤについては、利用範囲を拡大する見地からすると、認証に含まない方が望ましい。

【００２９】

図３では、入力データとしてＡ，Ｃ，Ｄ…が使用され、Ｂの使用が制限されている。計算処理では、コマンドａ，ｂ，ｄが処理されるが、コマンドｃの処理はされない。計算結果の内、出力データIとIIIは出力（利用者端末に返される）が、出力データIIは出力されない。ここで、特にコマンドは１つの処理方式を複数のコマンドに分けて制限すると共に、複数の処理方式から特定の処理方式を選ぶ、あるいは入力データや出力フォーマットに対応して特定の処理方式を選ぶような制限も加えて階層的に制限すると、より汎用性を持ったシステムが構築される。更に、要求される処理方式を持たない場合に、その処理方式を持つ他のシステムを探して、本リスク収益管理装置が他のシステムに対して利用者端末として接続し、計算処理結果を得るように構成すると、資源を共有した汎用システムが構築される。本発明の履歴認証による機密性の確保は、この場合に益々重要な機能となる。

【００３０】

尚、図３では、簡略化のために、入力データ、コマンド、出力データ共に、明確に分離されているように示したが、階層構造にしてどの階層までを利用可能に

する方法や、あるいはデータの一部にマスクをしたり、しなかったりを制御する方法、コマンド処理に関しては引数での制限、すなわちプログラム中で使用するパラメータの相違や分岐先の相違などによる制御も考えられる。更に、データの有効桁数の制限、計算での収束幅の制限、出力時にブランクや伏せ字に変更される等の制御による制限も可能である。本例において、このように利用者によって資源の利用やサービスを制限するのは、本システムを一般に公開するに際して、企業秘密や顧客の秘密などの機密データがインターネットなどを介して扱われることを考慮したためであり、機密の信頼性が高まるに応じて公開範囲を広くできるという関連がある。

【００３１】

図４は、入力データを管理するデータ管理データベース（ＤＢ）１ｂの概略構成例であり、入力データＡ，Ｂ，Ｃ，Ｄ…の内容が４１乃至４４で示されている。尚、図４のように入力データが明瞭に分離されることは少なく、上述した如く、各入力データＡ，Ｂ，Ｃ，Ｄ…がオーバーラップしているのが普通であり、実際には複雑に階層化されたり索引されたりしてデータベースが構造化されている。又、図４では、計算結果の出力データは示されていないが、出力データはデータ管理データベース（ＤＢ）１ｂに蓄積され、後に入力データとしても使用される。この場合の蓄積は、図３の出力データの制限に関係なく、全ての必要データが蓄積される。

【００３２】

図４のように、各データ領域４１～４４はヘッダとデータとから構成されており、ヘッダ部分には履歴認証キーが、例えば、何時、どの利用者が、このデータを登録したか、あるいはその利用者がこのデータの機密性のレベルや、具体的に誰には見せて良いか、誰には見せてはならないかなどが登録時又は更新時に記述され、上記図３の入力制限と相まって機密性を高めている。尚、データベースの機密性に応じて、図３と図４の履歴認証キーはその一方が使用されるものであってもよい。

【００３３】

図５は、計算処理プログラム２の一例を示す図である。

【００３４】

図５の例では、コマンドａ処理５１乃至コマンドｄ処理５４が示されている。図５においても、図４と同様に、各コマンド処理プログラム５１～５４にはヘッダが設けられ、この処理プログラムを使用可能な条件や、使用する場合の処理精度や処理方法に関わる情報が記述されている。

【００３５】

尚、図３の計算処理の制限の仕方は一例であって、例えば計算処理プログラム２での制限はコマンド対応でなく、各プログラムの引数で示され、モンテカルロ法などでの計算回数の制限をしてもよい。プログラムの引数の制御の具体例としては、離散型確率密度関数に準拠したモンテカルロ法と、連続型確率密度関数に準拠したモンテカルロ法とを用意し、プログラムの引数によって、両者の適用相手や範囲を制限するものも考えられる。

【００３６】

又、図３では、入力データ、計算処理、出力データの全てに制限を設けたが、出力データのみを制限し内部では必要な入力及び計算を全て行って、データ管理データベース（ＤＢ）１ｂに蓄積しておくようにしてもよい。このような場合には、利用者端末に返される出力データは制限に応じてマスクされ、企業名や顧客名、あるいは提供できないデータが伏せ字に置き代えられたものを返送して表示させるのが、営業効果を生む可能性があり好ましい。

【００３７】

＜本実施の形態の資産管理システムの動作例＞

以下、本実施の形態の資産管理システムの動作例を示す。尚、利用者端末６での動作、及びネットワークを介するやりとりや、データ圧縮・暗号化などは、本発明の主要部分ではないので、詳細には説明しない。

【００３８】

図６は、本実施の形態のリスク収益管理装置の全体の処理を示すフローチャートである。

【００３９】

リスク収益管理装置は、ステップＳ１０で、利用者端末６からのリクエストを

待つ。リクエストを受けると、ステップＳ２０で利用者端末６からのデータを受信する。この時に、端末や利用者の一次認証や、データの暗号解読と圧縮の展開なども行われる。尚、ここで、暗号化はデータの内容によって、その機密性に対応して異なる暗号化、あるいは機密性の高いものには複数の暗号化を行うなどの処理をするのが好ましい。特に、資産データは外部に漏れることを防ぐ必要があり、企業名や顧客名と共に最も厳しい暗号化が行われる。同様に、返送されるリスク収益管理データに対しても最も厳しい暗号化が行われる。

【００４０】

ステップＳ３０に進んで、図７で説明する履歴認証処理を行う。この履歴認証処理では、上述の利用者による制限が与えられる。ステップＳ４０では、制限をもとに入力データ及び／又は処理コマンドがせされ、図８で示すリスク変動・収益の計算処理が行われる。ステップＳ５０では、計算結果のリスク変動・収益管理データがリスク収益管理装置から利用者端末６に返される。利用者端末６はこのリスク収益管理データを表示する。尚、この表示フォーマットは、リスク収益管理装置が利用者端末６にダウンロードして提供するものであっても（この場合には、上記利用者への制限が表示フォーマットにも適用される）、利用者端末で独自に開発されたものでも構わない。

【００４１】

図７は、図６のステップＳ３０の履歴認証処理の一例を示すフローチャートである。

【００４２】

まず、ステップＳ３１では、利用者端末６から送られたデータから、端末ＩＤや利用者ＩＤが取得される。上述の如く、端末ＩＤは使用されない場合も多い。次に、ステップＳ３２で、履歴認証キーが取得される。ステップＳ３３では、取得された端末ＩＤや利用者ＩＤ、履歴認証キーに基づいて、利用者の「権限」が取得される（図３参照）。ステップＳ３４では、この取得された「権限」に変更がなされるかを判断し、変更がなければステップＳ３６に飛んで、「権限」を表わすデータを計算処理プログラムに渡す。ステップＳ３４で変更ありと判断されれば、ステップＳ３５で「権限」を変更して、ステップＳ３６で、変更された「

権限」を表わすデータを計算処理プログラムに渡す。尚、「権限」の変更は、金融機関間の関係や、取引額の変化や取引継続年月の長さ、などに基づいて、し尿レベルの変化に応じて逐次おこなわれる。従って、信用レベルの低下によって「権限」が制限されることもある。又、「権限」を、利用者ＩＤや履歴認証キーに対して固定して、再契約時に利用者ＩＤや履歴認証キーを変更するようにして制御してもよい。

【００４３】

図８は、図６のステップＳ４０の計算処理の一例を示すフローチャートである。この例では、入力データ、計算処理、出力データの全てで制限を行う例を示している。

【００４４】

まず、ステップＳ４１で、ステップＳ３０の結果の「権限」データを取得する。ステップＳ４２では、「権限」データに従って入力データを制限する。ステップＳ４３では、「権限」データに従って計算処理を制限する。ステップＳ４４では、上記入力データと計算処理の制限の下で資産変動やリスク管理の計算処理を実行する。ステップＳ４５では、計算結果の内から「権限」データに応じた情報を選択、あるいはマスクして出力する。

【００４５】

【発明の効果】

以上説明したように、本発明によれば、地理的に分散した利用者及び管理対象資産のデータを対象とした場合であっても、効率的かつ安全な資産のリスク管理及び収益管理を可能となる。

【００４６】

このため、データ量が大きな大手事業法人や顧客情報や信用情報が含まれるなど機密性の高い金融データを扱う金融機関であっても、低コストで開放されたネットワーク回線、例えばインターネット接続を通して資産のリスク管理及び収益管理機能が実現できるようになる。

【００４７】

又、バリュー・アット・リスク、リスク・リターン分析、ポートフォリオ最適

化など、個別の方法論において様様な見解や手法の相違が含まれるポートフォリオ理論を適用する場合は、利用者又は管理対象資産毎の履歴認証情報をもとにして別々の方式や異なる基準をあたかも異なるシステムを操作したかのように機能提供することができる。

【００４８】

加えて、持続的な機能向上や改定を行う場合も、地理的に分散した利用者端末の側はそのままにしておき、集中して設置されたリスク・収益管理装置の側を修正することで対応ができる。このため機能の維持コストや改定コストが低下する効果がある。

【図面の簡単な説明】

【図１】

本実施の形態の資産管理システムの構成例を示すブロック図である。

【図２】

本実施の形態の資産管理システムのハードウエア構成例を示すブロック図である。

【図３】

本実施の形態の履歴認証キーＤＢの一構成例を示す図である。

【図４】

本実施の形態のデータ管理ＤＢの一構成例を示す図である。

【図５】

本実施の形態の計算処理プログラムの一構成例を示す図である。

【図６】

本実施の形態のリスク収益管理装置の処理手順例を示すフローチャートである。

【図７】

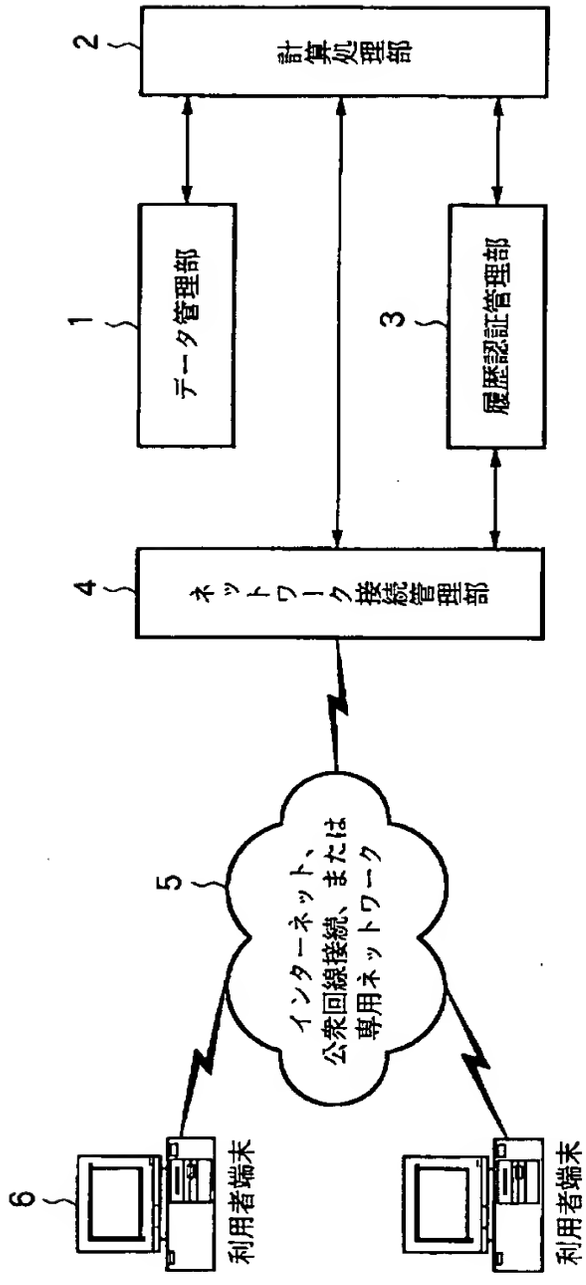
図６の履歴認証処理の処理手順例を示すフローチャートである。

【図８】

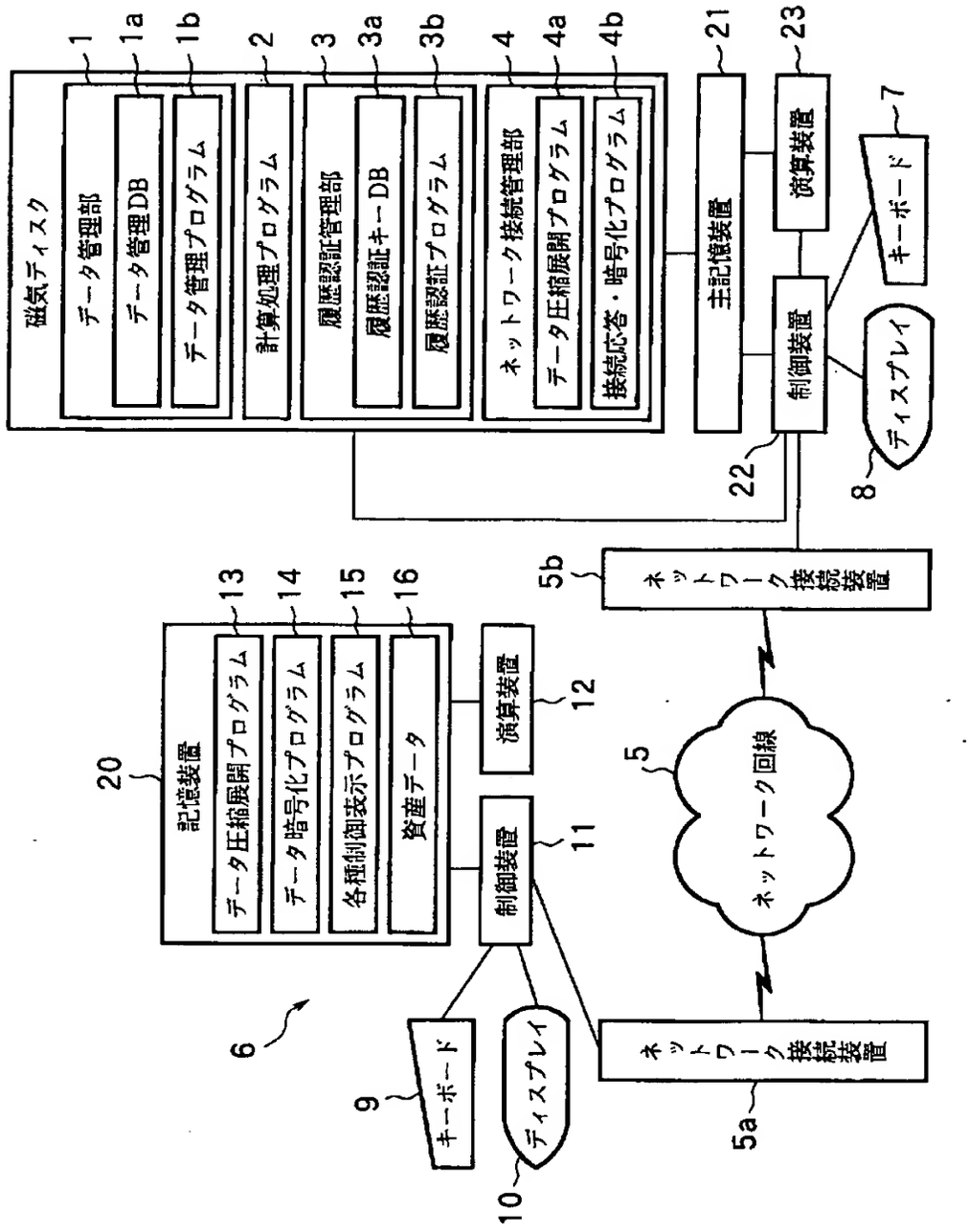
図６の計算処理の処理手順例を示すフローチャートである。

【書類名】　　図面

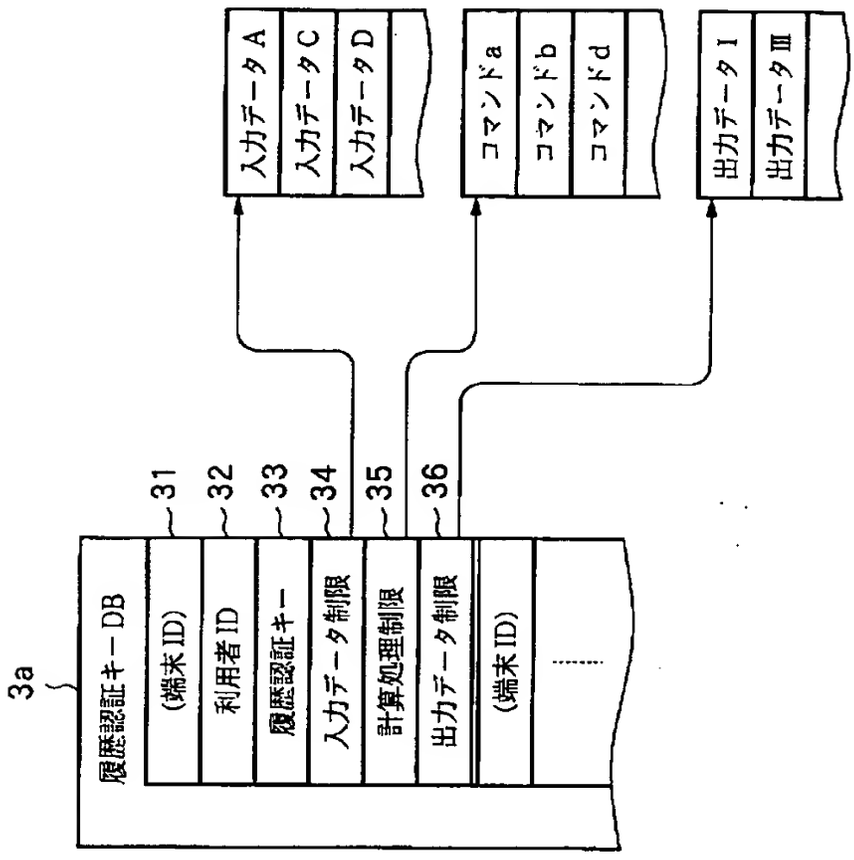
【図１】


2
計算処理部
1
データ管理部
3
履歴認証管理部
4
ネットワーク接続管理部
5
インターネット、
公衆回線接続、または
専用ネットワーク
6
利用者端末
利用者端末

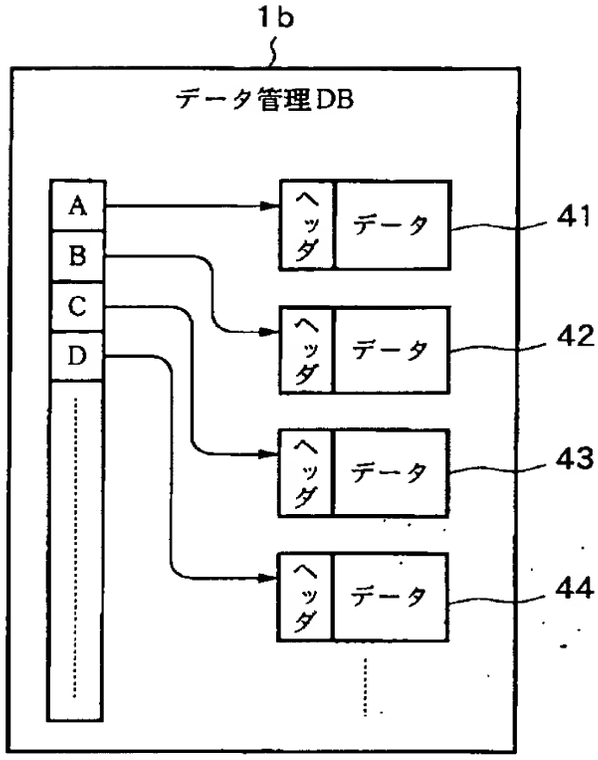
【図２】


磁気ディスク
1
データ管理部
1a
データ管理DB
1b
データ管理プログラム
2
計算処理プログラム
3
履歴認証管理部
3a
履歴認証キーDB
3b
履歴認証プログラム
4
ネットワーク接続管理部
4a
データ圧縮展開プログラム
4b
接続応答・暗号化プログラム
21
主記憶装置
23
演算装置
7
キーボード
制御装置
22
ディスプレイ
8
5b
ネットワーク接続装置
20
記憶装置
13
データ圧縮展開プログラム
14
データ暗号化プログラム
15
各種制御表示プログラム
16
資産データ
演算装置
12
制御装置
11
5
ネットワーク回線
6
9
キーボード
ディスプレイ
10
ネットワーク接続装置
5a

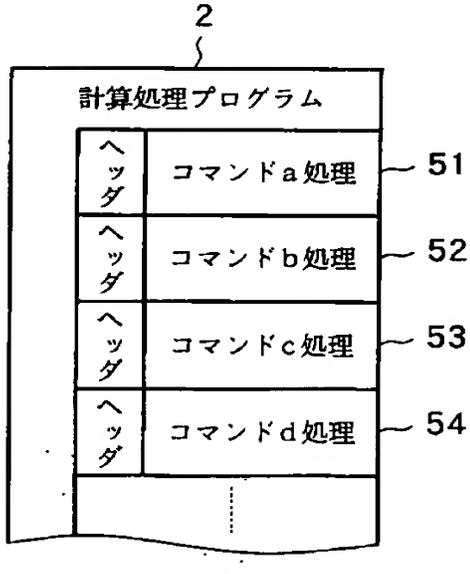
【図３】


入力データA
入力データC
入力データD
コマンドa
コマンドb
コマンドd
出力データI
出力データIII
3a
履歴認証キーDB
(端末ID)
利用者ID
履歴認証キー
入力データ制限
計算処理制限
出力データ制限
(端末ID)
31
32
33
34
35
36

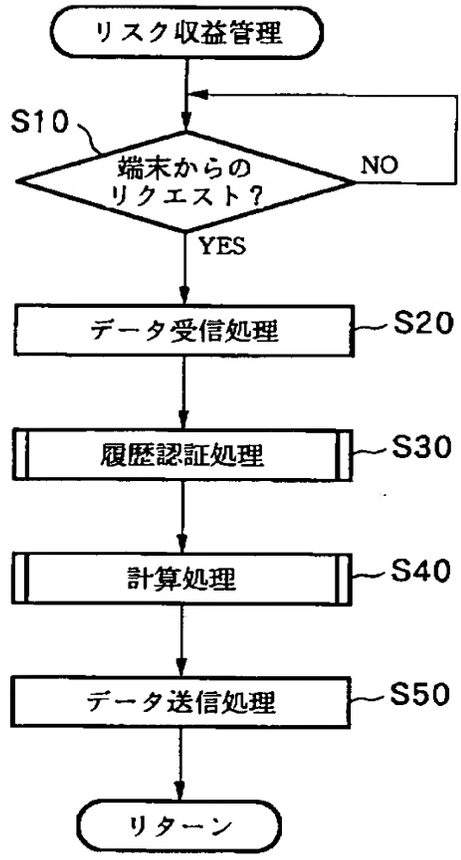
【図４】


1b
データ管理DB
A
B
C
D
ヘッダ
データ
41
42
43
44

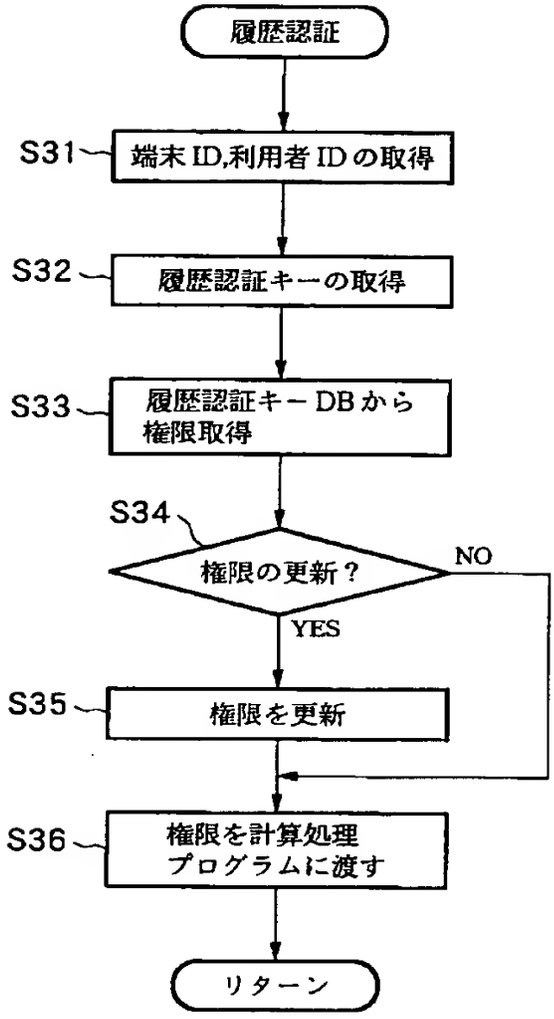
【図５】


2
計算処理プログラム
ヘッダ
コマンドａ処理
51
コマンドｂ処理
52
コマンドｃ処理
53
コマンドｄ処理
54

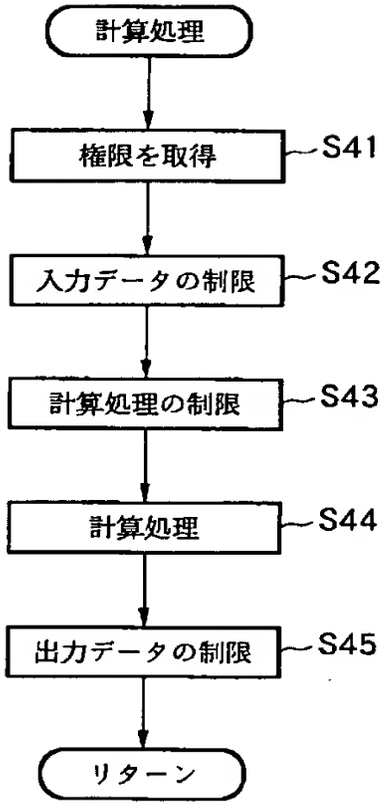
【図６】


リスク収益管理
S10
端末からの
リクエスト？
NO
YES
データ受信処理
S20
履歴認証処理
S30
計算処理
S40
データ送信処理
S50
リターン

【図７】


履歴認証
S31
端末ID,利用者IDの取得
S32
履歴認証キーの取得
S33
履歴認証キーDBから
権限取得
S34
権限の更新？
NO
YES
S35
権限を更新
S36
権限を計算処理
プログラムに渡す
リターン

【図８】


計算処理
権限を取得
S41
入力データの制限
S42
計算処理の制限
S43
計算処理
S44
出力データの制限
S45
リターン

【書類名】　　要約書

【要約】

【課題】　インターネット接続に代表される帯域が限定され信頼性と安全性に乏しいネットワーク間通信を利用して、地理的に分散した利用者及び管理対象資産のデータを対象に、利用者又は管理対象資産毎に別々の方式や異なる基準に基づいた資産のリスク管理及び収益管理を行う。

【解決手段】　集中して設置されるリスク収益管理装置と、地理的に分散した利用者端末との間でやりとりするデータを圧縮し、暗号化し、かつ利用者毎又は管理対象資産毎に認証キーを付加し、利用者毎又は管理対象資産毎に別々の方式や異なる基準に基づく出力結果をリスク収益管理装置から利用者端末に流す。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－１９９２７６
受付番号	５００００８２７２３８
書類名	特許願
担当官	塩崎　博子　　１６０６
作成日	平成１２年　７月１３日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　399070859

【住所又は居所】　東京都文京区本郷３－４２－５　ボア本郷４階

【氏名又は名称】　ニューメリカルテクノロジーズ株式会社

【代理人】　申請人

【識別番号】　100076428

【住所又は居所】　東京都千代田区紀尾井町３番６号　秀和紀尾井町パークビル７Ｆ　大塚国際特許事務所

【氏名又は名称】　大塚　康徳

【選任した代理人】

【識別番号】　100101306

【住所又は居所】　東京都千代田区紀尾井町３番６号　秀和紀尾井町パークビル７Ｆ　大塚国際特許事務所

【氏名又は名称】　丸山　幸雄

【選任した代理人】

【識別番号】　100115071

【住所又は居所】　東京都千代田区紀尾井町３番６号　秀和紀尾井町パークビル７Ｆ　大塚国際特許事務所

【氏名又は名称】　大塚　康弘

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９９０７０８５９〕

１．変更年月日　　１９９９年　９月　１日
　［変更理由］　新規登録
　　住　所　　東京都文京区本郷３－４２－５　ボア本郷４階
　　氏　名　　ニューメリカルテクノロジーズ株式会社